No title available.

Patent Number: ☐ DE19622533

Publication date: 1997-12-11

Inventor(s): SCHAEFER-LORINSER FRANK (DE); SCHEERHORN ALFRED (DE)

Applicant(s):: DEUTSCHE TELEKOM AG (DE)

Requested Patent: ☐ EP0909434 (WO9746983), B1, A3

Application Number: DE19961022533 19960605

Priority Number(s): DE19961022533 19960605

IPC Classification: G07F7/10 ; G06F12/14 ; G06F17/60

EC Classification: G07F7/08C, G07F7/10D4E2, H04L9/32B

Equivalents: AU3032197, CA2244126, CN1221507, JP2000512043T, ☐ WO9746983

Abstract

The problem associated with data security during payment transactions using smart cards lies in the processes involved in loading input data into an algorithm during authentication. According to the invention, the security of the withdrawal and charging data is improved by dividing the data blocks and switching an additional feedback to the downstream counters on and off at pre-selected times (cycles). The invention can be used in all authentication processes involving smart cards.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 22 533 A 1**

(51) Int. Cl.[6]:
G 07 F 7/10
G 06 F 12/14
G 06 F 17/60

(21) Aktenzeichen: 196 22 533.7
(22) Anmeldetag: 5. 6. 96
(43) Offenlegungstag: 11. 12. 97

DE 196 22 533 A 1

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(72) Erfinder:
Schaefer-Lorinser, Frank, 64372 Ober-Ramstadt, DE;
Scheerhorn, Alfred, 64293 Darmstadt, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 41 19 924 A1
DE 38 18 960 A1
EP 06 24 839 A1
EP 06 16 429 A1
EP 06 05 070 A2
WEIMANN,Jürgen: Risiken und Sicherheitspotentiale der Chipkarte. In: CR 12,1988, S.1037-1041;

(54) Verfahren und Vorrichtung zum Laden von Inputdaten in einen Algorithmus bei der Authentikation

(57) Die Problematik der Datensicherheit beim Zahlungsverkehr mit Hilfe von Chipkarten liegt in den Vorgängen beim Laden von Inputdaten in einen Algorithmus bei der Authentikation begründet.
Mit Hilfe einer Aufteilung der Datenblöcke und der Ein- und Ausschaltung einer zusätzlichen Rückkopplung nach den nachgeschalteten Zählern zu vorgewählten Zeiten (Takten) wird die Sicherheit der Ab- und Aufbuchungs-Daten verbessert.
Die Anwendung der Erfindung ist bei allen Authentikationsvorgängen in Verbindung mit Chipkarten möglich.

DE 196 22 533 A 1

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren, wie im Oberbegriff des Patentanspruch 1 näher beschrieben und auf eine Vorrichtung der im Oberbegriff des Patentanspruch 9 definierten Art. Verschiedene bekannte Verfahren dieser Art werden für Chipkarten mit Börsenfunktion in mehreren Varianten verwendet und bei den Vorrichtungen kann u. a. von Chipschaltungen entsprechend EP 0 616 429 A1 ausgegangen werden.

Verfahren der hier gemeinten Art sind z. B. aus ETSI D/EN/TE 090114, Terminal Equipment (TE) Requirements for IC cards and terminals for telecommunication use, Part 4 — Payment methods Version 4 v. 07. Febr. 1992 und aus der Europäischen Patentanmeldung 0 605 070 bekannt.

Neben Telefonkarten mit definiertem Anfangsguthaben als Zahlungsmittel für Kartentelefone sind auch "elektronische Geldbörsen" nach dem gleichen Prinzip als Zahlungsmittel für begrenzte Beträge von zunehmender Bedeutung. Für den Anwendungsfall "Bezahlen mit der Chipkarte" ist ein entsprechendes Kartenlesermodul mit einem Sicherheitsmodul SM zur Karten- und Guthabenprüfung in den Automaten gekoppelt.

Aus der EP 0 605 070 A2 ist auch ein Verfahren zum Transferieren von Buchgeldbeträgen auf und von Chipkarten bekannt, bei dem überschreibbare Speicherplätze einer Chipkarte aufgeteilt werden in wenigstens zwei Speicherplätze, von denen einer als "debitorisch", also "elektronische Geldbörse" genutzt wird, so wie die Telefonkarten, und der andere "kreditorisch" im Sinne einer Kreditkarte. Unter den für Kreditkarten üblichen gesicherten Bedingungen ist es vorgesehen, Geldbeträge zwischen den Bereichen zu transferieren, um die "elektronische Geldbörse" wieder aufzufüllen.

Zur Vermeidung sowohl der Gefahren unbefugter Zugriffe auf die Kassenautomaten und deren fest im Gerät integrierte Sicherheitsmodule, als auch der Notwendigkeit von besonders geschützten und deshalb für den Betreiber teuren Standleitungen wurde mit (P95114) ein Verfahren vorgeschlagen, bei dem vom Betreiber des Kassenautomaten vor den Kassiervorhängen ein Sicherheitsmodul mit Chipkartenfunktionen in die Kassenautomaten eingesteckt wird und bei jedem Kassiervorgang, bei dem ein Kartennutzer seine Chipkarte mit Börsenfunktion in einen Kassenautomaten eingesteckt hat, zuerst Datenbereiche der Chipkarte für eine Plausibilitätskontrolle und die Prüfung des Restguthabens ausgelesen, danach eine Authentifikation mit dem Sicherheitsmodul und eine ein-/mehrmalige Akzeptanzentscheidung durchgeführt werden und bei dem zuletzt der fällige bzw. eingegebene Geldbetrag aus der Chipkarte des Kartennutzers mit Hilfe einer Sicherheitsfunktion ab- und einem Summenzähler für Geldbeträge im Sicherheitsmodul aufgebucht werden und bei dem nach den Kassiervorgängen der Zählerstand des Sicherheitsmoduls mit Chipkartenfunktionen an eine Abrechnungszentrale übergeben wird.

Aufgabe der Erfindung ist es, die Sicherheit der Kassenautomaten für die "elektronischen Geldbörsen" gegenüber Manipulationen und Fehlfunktionen noch weiter zu erhöhen.

Diese Aufgabe löst ein Verfahren entsprechend dem Kennzeichen des Patentanspruchs 1.

Vorteilhafte Aus- bzw. Weiterbildungsmöglichkeiten dieses Verfahrens sind in den Kennzeichen der Unteransprüche 2 bis 8 aufgeführt.

Im Kennzeichen des Patentanspruchs 9 ist eine für die Anwendung des erwähnten Verfahrens geeignete Vorrichtung beschrieben.

Die Kennzeichen der Unteransprüche 10 bis 14 nennen vorteilhafte Aus- bzw. Weiterbildungsmöglichkeiten dieser Vorrichtungen für verschiedene Anwendungen

Die Erfindung ist mit ihren Wirkungen, Vorteilen und Anwendungsmöglichkeiten in den nachfolgenden Ausführungsbeispielen näher beschrieben.

Authentikationsalgorithmen werden i. A. zur sicheren Identifizierung verwendet. In Authentikationsverfahren gehen, neben der Identität von Chipkarten und Personen sowie evtl. eines Sicherheitsmoduls SM, oft noch weitere Daten ein, deren Korrektheit zusätzlich gesichert werden soll. Ein Authentikationsverfahren kann zum Beispiel auch auf nicht geheime Kartendaten D zusammen mit einem geheimen Schlüssel K und einer Zufallszahl Z angewendet werden. Bei den Chipkarten mit Börsenfunktion wird für die Ab- und Aufbuchungen sicherheitshalber je eine getrennte Sicherheitsfunktion verwendet, die jeweils mit einer kryptografischen Prüfsumme ausgelesen wird.

Mit dem Verfahren nach der Erfindung können die Ab- und Aufbuchungen mit einem kryptografischen Token durchgeführt werden, wobei vorausgesetzt wird, daß die Authentikation und die kryptografische Prüfsumme über den Zählerstand mit einem Challenge/Response-Verfahren durchgeführt werden. Dann kann durch ein einzelnes Challenge/Response-Verfahren, bei dem nur eine Zufallszahl von dem Sicherheitsmodul SM geliefert wird und von der Chipkarte nur eine Response berechnet wird, sowohl die Identität (Authentikation) als auch der interne Zählerstand gegenüber dem Sicherheitsmodul SM bewiesen werden.

Dies kann dadurch erreicht werden, daß die variablen Inputdaten, wie der Zählerstand und die Zufallszahl, intern jeweils zunächst mit "keyed Hashfunctions" = MAC Funktionen bearbeitet werden. Dabei wird als Schlüssel der kartenindividuelle geheime Schlüssel der Chipkarte verwendet. Die beiden aus Zählerstand und Zufallszahl gewonnenen Token können dann in — möglicherweise kryptografisch unsicherer Art — z. B. durch XOR oder ein linear rückgekoppeltes Schieberegister miteinander verknüpft werden und hiernach mit einer kryptografischen Funktion ausreichender Stärke integritätsgeschützt ausgegeben werden.

Diese Verfahrensweise ist für die Praxis dadurch interessant, daß die nur intern verwendeten keyed Hashfunctions keinen besonders hohen Ansprüchen hinsichtlich ihrer Sicherheit genügen müssen und relativ einfache Funktionen anwendbar sind, weil die Ergebnisse dieser Funktionen nicht aus der Chipkarte nach außen geführt werden. Dennoch werden damit Datenmanipulationen wirksam verhindert.

Das Ausführungsbeispiel der Erfindung geht von einem linear rückgekoppelten Schieberegister LFSR mit zusätzlicher nichtlinearer Funktion und nachgeschalteten Zählern aus:

0. Zusätzliche Rückkopplungen nach den nachgeschalteten Zählern in das linear rückgekoppelte Schieberegister LFSR werden geschaltet.

1. Es werden Inputdaten, bestehend aus den nicht geheimen Kartendaten D und dem geheimen Schlüssel K, in das linear rückgekoppelten Schieberegister LFSR eingelesen, während sowohl die Rückkopplung des linear rückgekoppelten Schieberegisters LFSR, als auch die zusätzliche(n) Rück-

kopplung(en) aktiv sind.
2. Es wird eine gewisse Anzahl von Takten weitergeschaltet, ohne daß zusätzliche Inputdaten eingelesen werden.
3. Es werden Inputdaten, bestehend aus der Zufallszahl R, eingelesen, während sowohl die Rückkopplung des LFSR, als auch die zusätzliche Rückkopplung(en) aktiv sind.
4. Es werden die zusätzlichen Rückkopplungen ausgeschaltet und ggf. die Zähler geändert.
5. Es wird eine gewisse Anzahl von Takten weitergeschaltet und während dieser Takte gemäß der aktuellen Zählerstände Outputbits erzeugt.

Patentansprüche

1. Verfahren zum Laden von Inputdaten in einen Algorithmus bei der Authentikation zwischen Chipkarten mit Börsenfunktion und einem Sicherheitsmodul, bei dem der Kartennutzer über ein gespeichertes Guthaben verfügen kann und bei dem bei jedem Kassiervorgang der erforderliche, bzw. der vom Kartennutzer eingegebene Geldbetrag aus der Chipkarte des Kartennutzers mit Hilfe einer Sicherheitsfunktion abgebucht und die Geldbeträge in einem Summenzähler für Geldbeträge des Sicherheitsmoduls aufaddiert und gespeichert werden, und bei dem für den Authentikationsalgorithmus ein linear rückgekoppeltes Schieberegister verwendet wird, dessen nichtlineare Funktionen in Verbindung mit nachgeschalteten Zählern kryptografisch verstärkt wird, und bei dem Inputdaten, wie z. B. eine Zufallszahl, ein geheimer Schlüssel und nicht geheime Kartendaten, in diesen Algorithmus eingehen, **dadurch gekennzeichnet,** daß die Inputdaten in mehrere Blöcke von Daten aufgeteilt werden und daß während des Ladens der Blöcke in das linear rückgekoppelte Schieberegister eine zusätzliche weitere Rückkopplung nach den nachgeschalteten Zähler in das Schieberegister eingeführt und nach einer vorgegebenen Anzahl von Taktschritten abgeschaltet wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Kartendaten D mit einem geheimen Schlüssel K als ein erster Block und eine Zufallszahl R als ein weiterer Block eingeführt werden.
3. Verfahren nach Anspruch 1 und 2, dadurch gekennzeichnet, daß während der Ladephase der Inputdaten andere Zählerstände eingesetzt werden, als bei der darauffolgenden Phase nach Einladen der Inputdaten zur Berechnung des Authentikationstokens.
4. Verfahren nach Anspruch 1 und 2, dadurch gekennzeichnet, daß der erste nachgeschaltete Zähler auf 1 zählt.
5. Verfahren nach Anspruch 1 und 2, dadurch gekennzeichnet, daß die Zähler und die Anzahl der auszuführenden Takte genau so gewählt werden, daß das Authentikationstoken nach einer durch andere Systembedingungen fest vorgegebenen Anzahl von Takten errechnet wird.
6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Ausgabe von Bits nach Einladen aller Inputdaten beginnt.
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß zwischen dem Einladen der Blöcke aus Anspruch 1 unter Beibehaltung der zusätzlichen Rückkopplung die gesamte Schaltung einige Schritte weiter getaktet wird, ohne daß Inputdaten geladen werden und bevor Bits ausgegeben werden.
8. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß zwischen dem Einladen der Blöcke aus Anspruch 1 nach Abschalten der zusätzlichen Rückkopplung die gesamte Schaltung eine bestimmte Anzahl von Schritten weiter getaktet wird, ohne daß Inputdaten geladen werden und bevor Bits ausgegeben werden.
9. Vorrichtung zum Laden von Inputdaten in einen Algorithmus bei der Authentikation unter Verwendung einer kryptografischen MAC Funktion, bestehend aus einem linear rückgekoppelten Schieberegister mit einer nichtlinearen "Feed Forward" Funktion, die aus dem Schieberegister abgreift und über einen Zähler den Output des Schieberegisters beeinflußt, dem ein weiterer Zähler nachgeschaltet ist, dadurch gekennzeichnet, daß die aus dem linear rückgekoppelten Schieberegister aufgebaute Schaltung mit nachgeschalteten Zählern zur Verwendung für den Authentikationsalgorithmus durch eine zusätzliche abschaltbare nichtlineare Rückkopplung kryptografisch verstärkt ist.
10. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die zusätzliche Rückkopplung nach dem ersten nachgeschalteten Zähler vor dem Latch abgegriffen ist.
11. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die zusätzliche Rückkopplung aus dem Latch nach dem ersten nachgeschalteten Zähler abgegriffen ist.
12. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die zusätzliche Rückkopplung nach dem zweiten nachgeschalteten Zähler abgegriffen ist.
13. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die zusätzliche Rückkopplung als eine XOR-Summe der Abgriffe nach dem ersten nachgeschalteten Zähler vor dem Latch, aus dem Latch nach dem ersten nachgeschalteten Zähler und nach dem zweiten nachgeschalteten Zähler ausgebildet ist.
14. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die Zähler aufgeteilt bzw. verkleinert sind.

- Leerseite -